Financial

Industry

Resilience,

Security, &

Teamwork

RPC first

TABLETOP EXERCISE

After Action Report
September 2008

RPC first
REGIONAL PARTNERSHIP COUNCIL

Exercise Designers

The RPC*first* tabletop exercise was sponsored by the U.S. Department of the Treasury. The Treasury Department and the leadership of the financial sector's Regional Partnership Council (RPC*first*) worked together to develop the exercise and provide participants with an opportunity to explore disaster response and preparedness issues in a collaborative environment.

- **UNITED STATES DEPARTMENT OF THE TREASURY, OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND COMPLIANCE POLICY (OCIP)**
  - The Treasury Department is the Sector Specific Agency for the Banking and Finance Sector;
  - The Treasury Department, in collaboration with State and Federal financial regulators, develops and implements policies to protect and mitigate disruptions to the sector through the Financial and Banking Information Infrastructure Committee (FBIIC);
  - Coordinates the public-private sector coalition efforts to improve the security and resilience of the sector; and
  - Supports the formation and growth of regional coalitions in order to address homeland security issues requiring a common response by a local financial community.

- **REGIONAL PARTNERSHIP COUNCIL (RPC*first*)**
  - A council of regional coalitions within the financial sector; and
  - RPC*first* assists regional coalitions in:
    - Sharing lessons learned about how the coalitions can coordinate with local and State government;
    - Leveraging the relationships of the regional coalitions with one another to engage in business continuity and homeland security efforts effectively and efficiently.

Table of Contents

Introduction

Since 2003, regional coalitions of financial institutions have formed organically in various cities and States across the nation. These coalitions aim to improve the critical infrastructure protection of the financial services sector at the local and regional levels. They enable financial institutions located in close geographic proximity to voluntarily collaborate and cooperate on issues related to business continuity. Regional coalitions also engage non-financial institutions from the public and not-for-profit sectors as "strategic partners." The public sector partnerships are beneficial because they provide the financial sector with access to information about their communities' disaster response plans and current and potential threats. In return, the regional coalitions provide government with a single point of contact for the financial services sector in a specific region.

Locations of Established or Developing Regional Coalitions

RPC*first* (Regional Partnership Council for Financial Industry Resilience, Security, and Teamwork) is an umbrella organization for all of the regional coalitions. The mission of the council is to ensure that the regional coalitions share lessons learned about how they can coordinate with local and State government, and leverage their relationships with one another to engage in business continuity and homeland security efforts effectively and efficiently.

RPC*first* held its second annual in-person meeting in San Francisco on May 15th - 16th, 2008. Representatives from eleven established coalitions and two

additional regions attended, as did Federal Government representatives and members of the San Francisco area's emergency management agencies.

As part of this meeting, the Treasury Department sponsored a tabletop exercise. The exercise was designed to:

- Examine RPC*first* communication and collaboration requirements during an emergency incident; and
- Provide insights into strategies to enhance the preparedness and response across RPC*first.*

The exercise provided the participants with a chance to practice their responses to a realistic emergency scenario as employees of financial institutions, members of regional coalitions, and members of RPC*first*. The participants explored such disaster preparedness issues as the development of communications strategies and information sharing among coalition members, and the cascading impacts of disasters on the sectors upon which financial services rely. As a result of the exercise, the participants were able to generate recommendations for improving the disaster planning of financial institutions and for strengthening RPC*first* as an organization.

Document Purpose & Description

The purpose of this document is to summarize the content and structure of the RPC*first* tabletop exercise, and to describe the key insights that emerged during the participants' discussions. The document is not intended to assign tasks to any entity, but rather to describe possible next steps that RPC*first* may choose to take to address challenges. Statements made during the exercise are not attributed to any individual or organization in this document.

Exercise Summary

STRUCTURE

Members of regional coalitions throughout the United States participated in the exercise. Numerous public sector representatives also took part to promote the building of public-private relationships and to provide the regional coalitions with information regarding the public sector's response to events described in the exercise scenario. Public sector participants represented numerous Federal agencies, as well as State, county, and local emergency management agencies in the San Francisco area.

The exercise was divided into two phases, called "moves." At the start of each move, participants received information describing simulated events. Subsequently, participants received a set of questions designed to help guide their thinking as they considered possible reactions to the events. The questions focused on such issues as the critical actions the institutions would be taking, how and what the institutions would be communicating to their employees, customers, and vendors, and what information the organizations would need from the public sector entities.

Participants were asked to consider the situation as both their individual financial institutions and the regional coalitions to which their institutions belong. Participants were given the chance to discuss the scenario and their responses to the questions in small group sessions. Following the small group sessions, the entire group reconvened and shared their thoughts with one another.

Following the completion of the second move, participants identified the insights and lessons learned that were generated during the exercise moves and examined how they could be developed into next steps for RPC*first*. The next steps focused on enhancing RPC*first* so that it can serve as a better resource for its membership during a disaster such as that described in the scenario.

See Appendix A for a list of the organizations that participated in the exercise. See Appendix B for the questions that the participants considered.

SCENARIO

The exercise was designed to encourage participants to think not only about how they would respond immediately following a disaster, but also about what steps they would take to prepare for a potential crisis situation. Consequently, the move 1 scenario contained information regarding the threat of terrorist attacks. The information was vague, with no specific buildings listed as targets, nor

specific methods of attack described as likely. With only ambiguous information, the participants were challenged to consider the expenditure of resources that would be an effective and appropriate response to the situation.

In contrast to the uncertainty of the threat in move 1, move 2 described a series of coordinated terrorist attacks on numerous locations throughout the United States. Participants considered emergency response issues and the implementation of their disaster plans, as well as macro level impacts to their financial institutions, including effects on the Nation's economy and the influence of the media on public behavior.

The following are summaries of the exercise scenario for each move:

Move 1: Intelligence Regarding Potential Threats Obtained by Authorities

Move 1 was simulated to begin on August 2, 2008. The U.S. Government had just received intelligence from Pakistani officials that they had uncovered evidence of a planned Al Qaeda attack on the United States. In the next few days, further evidence emerged. It indicated that Al Qaeda aimed to disrupt the economy of the Nation through damage to some of the Nation's key industries and through disruption of consumer activities in several of the Nation's cities. The likely target of these attacks was a variety of locations, in particular those related to commerce, oil and gas, telecom, and financial activities.

Move 2: Numerous Terrorist Attacks Occur Throughout the Nation

Move 2 was simulated to begin on August 5, 2008. The scenario opened with an explosion in lower Manhattan. This explosion was followed in the next few hours by an explosion in the San Francisco financial district, the discovery of an unexploded explosive device at the Port of Seattle, and an explosion at a Houston oil refinery. The Department of Homeland Security raised the homeland security alert for the Nation to SEVERE and other major U.S. cities began to brace for attacks. Citizens stocked up on necessities and some began to flee urban areas. Although no group claimed responsibility, the highly coordinated nature of the attacks and the previous intelligence reports led law enforcement to strongly suspect that Al Qaeda was responsible.

See Appendix C for more information regarding the exercise scenario.

PARTICIPANT ACTIONS

Without detailed information as to the exact nature of the terrorist threat, the response activities were largely at the discretion of each individual organization

during Move 1. Consequently, actions varied greatly. Some institutions indicated that the only action they would take would be to closely monitor developments, while others increased the level of security around their buildings and instituted twice daily conference calls with their organizations' leaders. Much of the variation in response was dependent upon whether or not an organization was located in one of the cities listed as a likely target in the scenario. The graphic below contains the key actions described by participants, both as members of financial institutions and as representatives of regional coalitions.

Move 1 Actions	
As a financial institution	▸ Carefully monitor information in the press and information released by the Financial Services - Information Sharing and Analysis Center (FS-ISAC) ▸ Reach out to city and State governments to gather information about what they are doing ▸ Activate incident assessment teams and raise their awareness; contact each of the point people within business units ▸ Hold twice daily conference calls with the organization's leadership ▸ Increase security around the perimeters of facilities ▸ Run checks of internal communications systems (such as e-mail) so that they are less likely to fail during the potential emergency o Speak with the information technology department and request that it be on a heightened level of alertness for anything out of the ordinary (such as a latency in the system) ▸ Communicate with employees o Distribute a calming message saying that business should continue as usual at the current time, and that more information will be provided as soon as it is available o Set up a daily update system on a 1-800 telephone number ▸ Communicate with vendors o Examine responsibilities and needs of the financial institution, and prioritize the order in which vendors are contacted accordingly o Ask vendors how their operations are changing in response to the threat, and what would likely happen to their services in the event of an attack o Ask vendors if they have additional information about the threat. They might receive information first if they are part of the infrastructure o Explain that the facility is now checking IDs and not accepting unplanned deliveries o Make sure to communicate to vendors servicing both primary and backup facilities
As a regional coalition	▸ Post updates on the coalition's website ▸ In appropriate circumstances, serve as an information conduit between Federal agencies and financial institutions

During the discussion following the presentation of the move 2 scenario, participants from local emergency services agencies expressed that local and State governments would be taking aggressive actions by shutting down roads,

etc., to protect public safety and safeguard essential services. Consequently, not only would financial institutions need to react to the direct impacts of the attacks, but they would also have to take into account how other sectors would be reacting and the impact this would have on their operations. Participants identified the following key actions as they considered the complex situation described in the move 2 scenario.

Move 2 Actions	
As a financial institution	▸ Activate emergency plans ▸ Gather information on employee status; open bridge lines ▸ Reach out to local emergency response agencies for information ▸ Get situational updates and instructions to employees as quickly as possible o Let employees know the schedule for information updates and how the information will be distributed o Communicate to employees that the Nation's alert level has changed to Red o Make sure employees know what happens when the Nation goes from Orange to Red alert level o In most situations, institutions will be encouraging people to shelter-in-place in the immediate aftermath of an attack ▸ Communicate to the regional coalition the status of the institution
As a regional coalition	▸ Through positions in local emergency operations centers, participate in the community's response efforts ▸ Continue to post information on the coalition website ▸ Assist institutions in need of support in linking up with those with available resources ▸ Continue to serve as a conduit – in particular by providing information concerning the state of the local financial sector to the Treasury Department

Insights and Next Steps

Two types of insights emerged during the exercise. The first set of insights related to general issues that will affect financial institutions, and the regional coalitions of which they are members, during a situation such as that described in the exercise scenario. The second set of insights was developed during the final session of the exercise, when participants used the lessons learned from moves 1 and 2 to discuss how RPC*first* might be able to achieve its organizational goals. The insights and the steps that could be taken to address related challenges are explained in detail in the following pages.

GENERAL INSIGHTS

1. In advance of a crisis, financial institutions need to build relationships with their local emergency management agencies to become integrated into their region's emergency response efforts.
2. During disasters, financial institutions need to be aware that successfully implementing their disaster plans may be challenging, as employees may feel compelled to act for their personal safety and the safety of their families. To increase employees' adherence to plans, financial institutions need to honestly address this issue and make certain that their plans are realistic, flexible, and well-practiced with roles and responsibilities clearly delineated.
3. Financial institutions need to maintain effective, ongoing communications with their employees during a disaster situation to better counter any misinformation that may be inadvertently circulated by the media.

RPC*first* INSIGHTS

4. RPC*first* needs to develop more redundancy within the organization to ensure that it is able to continue to operate in disaster situations.
5. RPC*first* needs to explore improved methods of communication, both to encourage the exchange of information among its members during normal times and to enable emergency communications during and following crises.
6. RPC*first* needs to develop and institutionalize processes to better enable regional coalitions to learn from each other's experiences.

INSIGHT 1: Building Local Relationships

In advance of a crisis, financial institutions need to build relationships with their local emergency management agencies to become integrated into their region's emergency response efforts.

Participants noted that a lack of communication and coordination sometimes exists between financial institutions and their communities' emergency management agencies during crises. As a result of this lack of pre-coordination, problems may arise during an incident, such as credentialed, critical employees being refused entry into their places of business. Through the participants' discussions, it emerged that this deficiency in coordination may stem from a lack of understanding of the contributions that the financial sector can make to a region's long-term recovery and the necessity of its involvement in response efforts. Additionally, inadequate coordination may be a result of the financial sector not being involved in community response planning.

NEXT STEP

- Through or with the assistance of their regional coalitions, financial institutions should reach out to their public sector emergency response partners, such as city managers, emergency councils, and the mayor's office, to establish lines of communications.

  The lines of communication will, at a minimum, foster information exchange and emergency response during a disaster. Ideally, these relationships will grow into planning coordination. Participants noted that public agencies may be more receptive to efforts to engage in community response planning if financial institutions also coordinate with other private critical infrastructures. The institution will then be able to "bring more to the table." Consequently, institutions may want to coordinate with other local companies (telephone, electric, etc.) prior to contacting their local emergency management agencies.

INSIGHT 2: Increasing Disaster Plan Efficacy

During disasters, financial institutions need to be aware that successfully implementing their disaster plans may be challenging, as employees may feel compelled to act for their personal safety and the safety of their families. To increase employees' adherence to plans, financial institutions need to honestly address this issue and make certain that their plans are realistic, flexible, and well-practiced with roles and responsibilities clearly delineated.

Participants discussed that, in emergency situations, carefully developed plans may be circumvented by employees who opt to take individual actions over those recommended by their employers. One participant provided an example of employees rushing from their workplace to try to reach their children, while according to the institution's crisis response plans, employees were instructed to shelter-in-place. Such behavior may put an employee at greater risk than if he or she had stayed at the workplace. Consequently, institutions should take into account that such behavior will occur, while still striving to develop plans that will provide for the best outcomes for both employees and businesses. Disaster planning should also consider what steps can be taken to help improve employee observance of plans.

Next Steps

- Financial institutions should examine their existing plans to ensure they do not contain unrealistic expectations of employee behavior and that the current protocols contain contingency plans in the event that there is a lack of adherence to primary plans.
- Financial institutions should educate employees so that they are less likely to panic in disaster situations and take ill-considered actions. This education may include training employees in basic first aid skills, and instructing employees in the importance of personal/family emergency plans.
- Financial institutions should try to increase employee confidence in their institutions' plans. This can be accomplished through frequent testing of plans. Testing will not only familiarize employees with their roles and responsibilities and the actions that they will need to take, but it will also ensure that plans remain current.

INSIGHT 3: Communicating with Employees

Financial institutions need to maintain effective, ongoing communications with their employees during a disaster situation to counter misinformation that may be inadvertently circulated by the media.

Following an incident, the media may broadcast unsubstantiated information in their haste to report on a dramatic situation. Participants commented that the indications in the exercise scenario that terrorists were researching radiological materials would gain a lot of attention in the media and possibly contribute to public anxiety. In such a situation, financial institutions will need to strive to overcome the public anxiety in order to keep their employees calm and accurately informed.

Next Steps

- Financial institutions should let employees know how they will provide information and how frequently it will be updated during an incident. Available methods of communication and the frequency of updates will depend on the nature of the incident. Ideally, institutions will provide as much substantiated information as possible to employees in a timely manner. Institutions should also let employees know when there is no additional information to be provided at the current time. These protocols will help to ensure that employees will view their employers as trusted information sources and minimize the influence of inaccurate information.

INSIGHT 4: Developing Redundancy within RPC*first*

RPCfirst needs to develop more redundancy within the organization to ensure that it is able to continue to operate in disaster situations.

RPC*first* is currently relying on two individuals located in the same city to coordinate all aspects of the council. Participants raised concerns that RPC*first* may not be able to function in the event that an emergency occurs in that city.

Next Step

- RPC*first* should identify first and second alternates who will be able to oversee the council's activities if needed. These alternates might be the heads of regional coalitions who have indicated that they would be willing to assume that responsibility.

INSIGHT 5: Improving RPC*first*'s Communications

RPCfirst needs to explore improved methods of communication, both to encourage the exchange of information among its members during normal times and to enable emergency communications during and following crises.

RPC*first* does not currently have an established system for regular communications with its membership. Establishing communication systems will enable more frequent dialog, strengthen the council, and provide a valuable resource for its membership. For example, the exchange of information will be useful as the institutions within a coalition are determining their course of action during a disaster. They will be able to discover the actions of coalitions across the country and make a more informed decision.

Next Steps

- RPC*first* could create an email distribution list that includes all of the regional coalitions. This action would enable individual coalitions to more easily reach out to others to distribute or request information.
- RPC*first* may wish to develop a blog, which may encourage informal and frequent discussions between members. RPC*first*'s leadership could post relevant articles to spur discussions or let members choose topics on which they are seeking input from other regional coalitions.
- During a time of crisis, RPC*first* could use a commercially available alert system, such as those that some individual regional coalitions employ. This may help when normal means of communication may be inoperable. An alert system could provide brief updates and instruct members as to when and where they should go for further information.

INSIGHT 6: Enabling Coalitions to Learn From Each Other Through RPC*first*

RPCfirst needs to develop and institutionalize processes to better enable regional coalitions to learn from each other's experiences.

The members of RPC*first* have a wealth of different experiences, both due to their different geographic locations and to their varying levels of development as regional coalitions. As a council of coalitions, RPC*first* is uniquely positioned to serve as the central repository for the acquired knowledge of the regional coalitions, facilitating learning across coalitions.

Next Step

- RPCfirst's leadership should gather the lessons learned from regional coalitions that have experienced a disaster. These lessons could include emergency measures that were successful and those that were not effective. It may also include the actions that financial institutions and regional coalitions would do differently if confronted with a similar situation again. With this information, RPC*first* would be able to communicate best practices from financial institutions and coalitions across the nation and ensure the sharing of valuable information.

RPC *first*

TABLETOP EXERCISE

Appendices

APPENDIX A:

EXERCISE PARTICIPANTS
The following is a list of the organizations that participated in the exercise.

Private Sector Participants

- ArizonaFIRST (State of Arizona)
- BARCfirst (San Francisco Bay area (north, east, and south of the bay))
- Central California
- ChicagoFIRST (Chicago and surrounding counties)
- dfwFIRST (Dallas-Ft. Worth Metroplex, including four surrounding counties)
- FloridaFIRST (State of Florida)
- HawaiiFIRST (State of Hawaii)
- Las Vegas (City of Las Vegas)
- Minnesota Information Sharing & Analysis Center (State of Minnesota)
- NCRfirst (National Capitol Region: Washington, D.C, and parts of Maryland and Virginia)
- Financial Recovery Coalition of North Carolina (State of North Carolina)
- SoCalfirst (Southern California - Los Angeles, Orange, Riverside, San Bernardino, Ventura, Kern, and Santa Barbara counties)
- WashingtonFIRST (State of Washington)

Public Sector – Federal

- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Office of the Comptroller of the Currency
- U.S. Department of Homeland Security (DHS)
- U.S. Department of the Treasury

Public Sector – State, County, and Local

- Marin County Sheriff Office of Emergency Services
- San Bruno Fire Department
- San Francisco Fire Department
- San Mateo County Department of Public Health
- San Mateo County Office of Emergency Services
- State of California Office of Emergency Services

APPENDIX B:

QUESTIONS FOR CONSIDERATION DURING THE EXERCISE

Following the presentation of each scenario move, the participants were asked to consider the following questions. The exercise concluded with an insights and next steps session.

Move 1 and Move 2 Questions
As a financial institution: ▸ What are your concerns and what critical actions are you taking now? ▸ How and what are you communicating to your institution's employees, vendors and customers? As a regional coalition: ▸ How are you coordinating and communicating with members of your regional coalition? ▸ What information would be valuable to hear from your coalition members (as the head of the coalition or as a member)? ▸ How and what are you communicating to other regional coalitions? ▸ What information would be helpful from other regional coalitions? ▸ What information do you need from Federal, State, and local authorities?

Insights and Next Steps Questions
▸ What is the role of RPC *first* during a crisis? ▸ What is the role of your individual coalition during the crisis? ▸ What is not currently in place that needs to be in order to fulfill your role? ▸ What are the next steps for RPC *first*?

APPENDIX C:

EXERCISE SCENARIO
During the exercise, the simulated date was August 2008. The participants received the following scenario information.

Move 1: Intelligence Regarding Potential Threats Obtained by Authorities

- August 2, 2008: A Pakistani government raid on a suspected Al Qaeda terrorist training camp on the Pakistan-Afghanistan border gleaned credible evidence that plans for an attack had been in progress for months and aimed to hit the U.S. in the coming week. Evidence suggested that Al Qaeda planned to operate through its network of supporter organizations within the U.S. Sources also indicated that the terrorists aimed to severely disrupt the Nation's economy through damage to some of the Nation's key industries and through disruption of consumer activities. The targets of these attacks were likely to be a variety of types of locations, in particular those related to commercial, oil and gas, telecom, and financial activities.

- August 3, 2008: Following complaints by a neighbor of late-night sightings of a group of 4-5 men at a nearby suburban self-storage facility, Jersey City Police initiated a review of access records and conducted a raid of the suspicious unit. The Homeland Infrastructure Threat and Risk Assessment Center (HITRAC) reported that documents seized in the raid appeared to outline methods of attack and vulnerable targets. Most of the documents consisted of detailed road maps, commuter train plans, and tourist maps of New York City, San Francisco, Houston, Los Angeles, and Boston. Promotional information from medical supply companies advertising cancer treatment equipment was also found, leading authorities to suspect that the terrorists may be intending to use elements used in cancer treatment to construct a radiological weapon. As a result of this information, DHS raised the threat level for the indicated cities to HIGH.

- August 4, 2008: The morning edition of *The Washington Post* led with the headline "Evidence of Terrorist Plot from Jersey City Raid." *The Post* obtained documents recovered from the self-storage facility which revealed detailed knowledge of the San Francisco metropolitan area. The documents obtained included information about telecommunications

Move 2: Numerous Terrorist Attacks Occur Throughout the Nation

- August 5, 2008, 11:05 AM ET: In New York, reports indicated that a Ryder truck had exploded directly in front of a building housing major Verizon equipment. It appeared to have been a massive explosion. The explosion destroyed a substantial part of the building, severely damaging the Verizon switches. As a result, there was no land-based phone service, and cell phone service and computer connections were interrupted in lower Manhattan. The Brooklyn Bridge also sustained some damage and was closed to all traffic and pedestrians.

- August 5, 2008, 8:42 AM PT: During the morning rush of employees arriving for work in San Francisco's financial district, an apparent bomb detonated within the Transamerica Pyramid building at 505 Sansome Street. One side of the building partially collapsed and scared bystanders were running in panic through the streets and pouring out of surrounding buildings. Police were canvassing the area searching for indications of the source of the attack. Initial reports from witnesses suggested that casualty rates would be very high.

- August 5, 2008, 12:00 PM ET: DHS raised the homeland security alert for the Nation to SEVERE.

- August 5, 2008, 12:15 PM ET: President Bush issued implementing instructions in accordance with the National Response Framework. President Bush and Michael Chertoff, the Secretary of Homeland Security, spoke in a televised speech to the Nation.

- August 5, 2008, 1:12 PM PT: A bomb was found in a shipping container that was being delivered to the Port of Seattle's Terminal 18. The truck carrying the container had overturned in an accident inside the gate. The device was discovered in a lead-lined box that had fallen open in the accident. The bomb was equipped with a GPS-enabled detonation device with a cell phone activated back-up detonator. The device would have allowed the terrorists to set the bomb to explode at a predetermined location (accurate to within 15 meters). If the GPS detonator had failed, or the container were rerouted, the cell phone back up would still have allowed the terrorists to detonate the device. The GPS detonator was damaged during defusing, so it was not clear where this bomb was set to detonate. Police questioned the driver and trucking company

representatives, but they claimed to have no knowledge of how the device came to be in their vehicle.

- August 5, 2008, 1:45 PM PT: The Port of Seattle was in lock-down, with all cargo movement frozen and only law enforcement allowed admittance. Ports around the country reacted to Seattle's near miss and port activities ground to a halt. Cargo remained in ships' hulls while ports determined their courses of action. Concern over the availability of goods, should the lock-down continue several days, was already being voiced by retailers.

- August 5, 2008, 3:50 PM CT: A huge explosion occurred at a Houston petrochemical refinery. A massive fireball was reported and the refinery was burning. Due to the possibility of toxic chemicals, individuals were evacuated from the area. The cause of the explosion could not yet be determined, but a security guard reported that a rental truck made an unauthorized entry into the facility minutes before the explosion took place. Authorities halted traffic through the Houston Ship Channel until they could ascertain that no further attacks on the city were imminent.

- August 5, 2008, 5:00 PM ET: Local news covering the attacks portrayed the series of events as a continuing terrorist plot to disrupt the American economy. Other major U.S. cities began to brace for an attack as citizens stocked up on necessities and some began to flee urban areas.

- August 6, 2008: Although no group had yet claimed responsibility, the highly coordinated nature of the attacks and the previous intelligence reports led law enforcement to strongly suspect that Al Qaeda was responsible. Similarities in the compositions of the explosive residues found at the attack sites and at the Port of Seattle supported the theory that one group was responsible. Evidence of ammonium nitrate/fuel oil, a readily available conventional explosive material, had been found in debris from each site. All of the attacks appeared to have used improvised explosive devices to detonate bombs. In the financial sector, the financial markets were significantly impacted by these events and there was a flight to quality. Trading restrictions were in effect.